AUTHENTICATION KEY DISTRIBUTION FOR MOBILE STATIONS

Publication number: RU2190310 (C2)
Publication date: 2002-09-27
Inventor(s): FENEL MAJKL DEHVID [US]
Applicant(s): EHRIKSSON INK [US]
Classification:
- international: ***H04W12/04; H04L29/06; H04W12/00; H04W12/06;*** *H04W12/02;* **H04L29/06; H04W12/00;** (IPC1-7): H04Q7/38
- European: H04L29/06S8; H04L29/06S6; H04Q7/38A; H04W12/04; H04W12/06
Application number: RU19990111365 19971027
Priority number(s): US19960739259 19961030

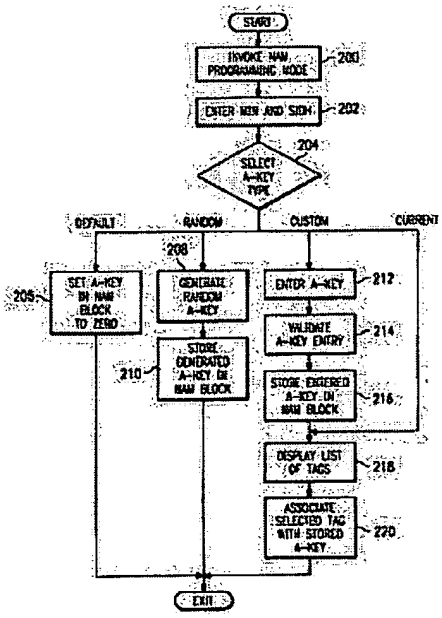
Also published as:

- WO9819493 (A2)
- WO9819493 (A3)
- US5887251 (A)
- KR20000052852 (A)
- EP0965240 (A2)

more >>

Abstract of **RU 2190310 (C2)**

wireless communication systems; authentication of mobile stations in cellular radio communication systems. SUBSTANCE: proposed method and device used for distributing authentication keys (A- keys) enable mobile stations to receive command entered by user for selecting A-key out of plurality of probable values saved in memory including value given by default and user-given client s value of A-key. In response to command mobile station can set A-key in its memory to value given by default or to internal generated or pre-saved random value, or to client s value entered by user. Command, irrespective of whether it is meant for selecting value set by default, random, or client s value, may be entered in the course of programming mobile station number assignment module. EFFECT: enhanced precision of channel adjustment. 20 cl, 4 dwg



(19) RU (11) 2 190 310 (13) C2

(51) МПК[7] H 04 Q 7/38

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 99111365/09, 27.10.1997

(24) Дата начала действия патента: 27.10.1997

(30) Приоритет: 30.10.1996 US 08/739,259

(46) Дата публикации: 27.09.2002

(56) Ссылки: US 5551073 A, 27.08.1996. RU 2090006 C1, 10.09.1997. RU 2060593 C1, 20.05.1996. US 5513245 A, 30.04.1996. WO 96/01536 A1, 18.01.1996. US 5239294 A, 24.08.1993. US 5091942 A, 25.02.1992. US 5227613 A, 13.07.1993.

(85) Дата перевода заявки PCT на национальную фазу: 31.05.1999

(86) Заявка PCT:
US 97/19662 (27.10.1997)

(87) Публикация PCT:
WO 98/19493 (07.05.1998)

(98) Адрес для переписки:
129010, Москва, ул. Большая Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", Ю.Д.Кузнецову, рег. № 595

(71) Заявитель:
ЭРИКССОН ИНК. (US)

(72) Изобретатель: ФЕНЕЛ Майкл Дэвид (US)

(73) Патентообладатель:
ЭРИКССОН ИНК. (US)

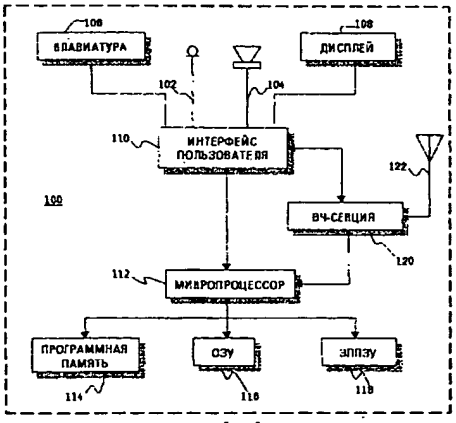
(74) Патентный поверенный:
Кузнецов Юрий Дмитриевич

RU 2190310 C2

(54) РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ АУТЕНТИФИКАЦИИ ДЛЯ МОБИЛЬНЫХ СТАНЦИЙ

(57)

Изобретение относится к системам беспроводной связи и, более конкретно, к способу и устройству для распределения ключей аутентификации (А-ключей), которые используют для аутентификации мобильных станций в сотовой системе радиосвязи. Технический результат - повышение точности настройки каналов. Настоящий способ позволяет мобильной станции принимать команду, вводимую пользователем для выбора из множества возможных значений ключа аутентификации (А-ключа), хранящегося в ее памяти, включающих в себя значение, задаваемое по умолчанию, случайное значение и клиентское (задаваемое пользователем) значение А-ключа. В ответ на команду мобильная станция может устанавливать А-ключ в своей памяти на значение, задаваемое по умолчанию, или на внутренне генерируемое или предварительно сохраненное случайное значение, или на клиентское значение, введенное пользователем. Команда, будь то для выбора задаваемого по умолчанию, случайного или клиентского значения, может вводиться в ходе программирования модуля присвоения номера (МПН) мобильной станции. 2 с. и 18 з.п. ф-лы, 4 ил.



Фиг. 2

RU 2190310 C2

(19) **RU** (11) **2 190 310** (13) **C2**

(51) Int. Cl.[7] **H 04 Q 7/38**

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 99111365/09, 27.10.1997

(24) Effective date for property rights: 27.10.1997

(30) Priority: 30.10.1996 US 08/739,259

(46) Date of publication: 27.09.2002

(85) Commencement of national phase: 31.05.1999

(86) PCT application:
US 97/19662 (27.10.1997)

(87) PCT publication:
WO 98/19493 (07.05.1998)

(98) Mail address:
129010, Moskva, ul. Bol'shaja Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", Ju.D.Kuznetsovu, reg. № 595

(71) Applicant:
EhRIKSSON INK. (US)

(72) Inventor: FENEL Majkl Dehvid (US)

(73) Proprietor:
EhRIKSSON INK. (US)

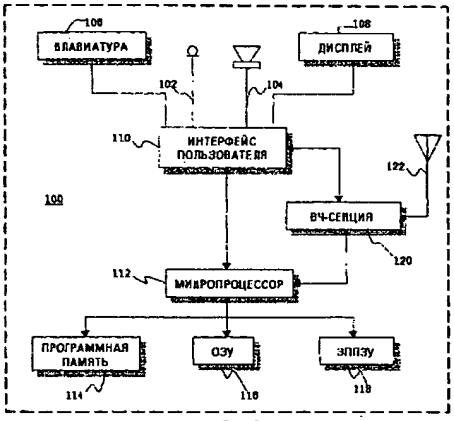
(74) Representative:
Kuznetsov Jurij Dmitrievich

(54) AUTHENTICATION KEY DISTRIBUTION FOR MOBILE STATIONS

(57) Abstract:

FIELD: wireless communication systems; authentication of mobile stations in cellular radio communication systems. SUBSTANCE: proposed method and device used for distributing authentication keys (A- keys) enable mobile stations to receive command entered by user for selecting A-key out of plurality of probable values saved in memory including value given by default and user-given client s value of A-key. In response to command mobile station can set A-key in its memory to value given by default or to internal generated or pre-saved random value, or to client s value entered by user. Command, irrespective of whether it is meant for selecting value set by default, random, or client s value, may be entered in the course of programming mobile station number assignment module.

EFFECT: enhanced precision of channel adjustment. 20 cl, 4 dwg



Фиг. 2

RU 2190310 C2

RU 2190310 C2

Область техники, к которой относится изобретение

Настоящее изобретение относится к системам беспроводной связи и более конкретно к способу и устройству для распределения ключей аутентификации (А-ключей), которые используют для аутентификации мобильных станций в сотовой системе радиосвязи.

Уровень техники

Уровень техники включает в себя сотовые системы радиосвязи, которые действуют в Соединенных Штатах с начала 1980-х годов, и предоставляют телефонное обслуживание непрерывно растущей абонентской базе, в настоящее время оцениваемой в более чем 20 миллионов абонентов. Сотовая телефонная служба действует во многом так же, как и стационарная проводная телефонная служба в жилых домах и в учреждениях, за исключением того, что для соединения телефонных вызовов к и от мобильных абонентов используются не телефонные провода, а радиочастоты. Каждому мобильному абоненту присваивается личный (10-значный) абонентский телефонный номер и ему обычно ежемесячно выставляют счет на основании количества "эфирного времени", которое он тратит, разговаривая по сотовому телефону. Многие из особенностей обслуживания, доступные пользователям наземной телефонной линии (например, ожидание вызова, переадресация вызова, трехсторонний вызов и т.д.), также, в основном, доступны абонентам мобильной связи.

В Соединенных Штатах лицензии на сотовую связь выдаются Федеральной комиссией связи (ФКС) в соответствии со схемой лицензирования, которая делит страну на географические рынки услуг, определяемые согласно Переписи 1980 г. На каждый рынок выдается только две лицензии на сотовую связь. Две сотовые системы в каждом рынке обычно именуют соответственно "системой А" и "системой Б". Каждой из двух систем выделяют отдельный частотный блок в полосе 800 МГц (именуемые соответственно А-полосой и Б-полосой). На сегодняшний день ФКС освободила для услуг сотовой связи в общей сложности 50 МГц (по 25 МГц на систему). Мобильные абоненты могут свободно абонировать услуги как у оператора системы А, так и у оператора системы Б (или у обоих). Каждая система присваивает каждому из своих абонентов мобильный идентификационный номер (МИН). Местная система, услуга которой абонируется, именуется "домашней" системой. При передвижении вне "домашней" системы мобильный абонент имеет возможность получать услуги в удаленной системе, если между операторам "домашней" и "гостевой" систем имеется соглашение по "роумингу".

Архитектура типичной сотовой системы радиосвязи изображена на фиг. 1. Географическая область (например, городской район) делится на несколько меньших, соприкасающихся зон обслуживания радиосвязи, именуемых "сотами", таких как, например, соты С1-С10. Соты С1-С10 обслуживаются соответствующими группами стационарных радиостанций, именуемых "базовыми станциями" Б1-Б10, каждая из которых включает в себя совокупность блоков ВЧ-канала (приемопередатчиков), которые работают на поднаборе ВЧ-каналов, присвоенных системе, как известно из уровня техники. В иллюстративных целях базовые станции Б1-Б10 изображены на фиг. 1 расположенными по центру сот, соответственно С1-С10, и показаны оборудованными всенаправленными антеннами, передающими одинаково во всех направлениях. Однако базовые станции Б1-Б10 могут также располагаться ближе к периферии или иным образом вне центров сот С1-С10 и могут направленно облучать высокочастотными сигналами соты С1-С10 (например, базовая станция может быть оборудована тремя направленными антеннами, каждая из которых покрывает сектор в 120°).

ВЧ-каналы, выделенные любой данной соте (или сектору), могут повторно выделяться удаленной соте в соответствии с принципом повторного использования частоты, известным из уровня техники. В каждой соте (или секторе) по меньшей мере один ВЧ-канал используется для переноса сообщений управления или контроля и называется каналом "управления" или "поискового вызова/доступа". Другие ВЧ-каналы используются для переноса голосовых переговоров и называются "голосовыми" или "речевыми" каналами. Пользователи сотовых телефонов (мобильные абоненты) в сотах С1-С10 снабжены портативными (ручными), передвижными (переносными) или мобильными (монтируемыми на автомобилях) телефонными блоками, носящими общее название "мобильные станции", примерами которых являются мобильные станции М1-М5, каждая из которых связывается с ближней базовой станцией. Каждая из мобильных станций М1-М5 включает в себя контроллер (микропроцессор) и приемопередатчик, известные из уровня техники. Приемопередатчик в каждой мобильной станции может настраиваться на любой из ВЧ-каналов, конкретизированных в системе (тогда как каждый из приемопередатчиков в базовых станциях Б1-Б10 обычно работает только на одном из различных ВЧ-каналов, используемых в соответствующей соте).

Как представлено на фиг. 1, базовые станции подключены к пункту 20 коммутации мобильных телефонов (ПКМТ) и принимают его управление. ПКМТ 20, в свою очередь, подключен к центральному пункту (не показан на фиг. 1) в коммутируемой телефонной сети 30 общего пользования (КТСОП) с наземными (проводными) линиями связи или к аналогичному средству обслуживания, например, к цифровой сети с интеграцией функций ЦСИФ. КТСОП 20 коммутирует вызовы между проводными и мобильными абонентами, управляет передачей сигналов на мобильные станции М1-М5, составляет статистику выставления счетов, хранит профили обслуживания абонента и обеспечивает работу, поддержание и тестирование системы.

При включении (подаче питания) каждая из мобильных станций М1-М5 переходит в свободное состояние (режим ожидания) и

RU 2190310 C2

RU 2190310 C2

настраивается на самый сильный канал управления (в общем случае канал управления соты, в которой в данный момент располагается мобильная станция) и непрерывно отслеживает его. При перемещении между сотами в свободном состоянии мобильная станция в конце концов "потеряет" высокочастотное соединение на канале управления "старой" соты и настроится на канал управления "новой" соты. Как первоначальная настройка на канал управления, так и его изменение выполняются автоматически, путем сканирования всех действующих каналов управления в сотовой системе, чтобы найти "наилучший" канал управления (в Соединенных Штатах в каждой сотовой системе имеется 21 "специализированный" канал управления, а это значит, что мобильная станция должна сканировать максимум 21 ВЧ-канал). Найдя канал управления с хорошим приемом, мобильная станция остается настроенной на этот канал, пока его качество снова не ухудшится. Таким образом, мобильная станция остается "на связи" с системой и может принимать или инициировать телефонный вызов через одну из базовых станций Б1-Б10, подключенных к ПКМТ 20.

Чтобы обнаружить входящие вызовы, мобильная станция непрерывно отслеживает текущий канал управления, чтобы определить, принято ли адресованное ей (т.е. содержащее ее МИН) сообщение системы поискового вызова. Сообщение системы поискового вызова посылается на мобильную станцию, например, когда обычный абонент (наземной линии связи) вызывает мобильного абонента. Вызов направляется из ЦСИФ 30 на ПКМТ 20, где набранный номер подвергается анализу. Если набранный номер признан допустимым, ПКМТ 20 запрашивает некоторые или все базовые станции Б1-Б10 на осуществление поискового вызова по соответствующим им сотам С1-С10 вызываемой мобильной станции.

Каждая из базовых станций Б1-Б10, принимающих запрос от ПКМТ 20, будет затем передавать по каналу управления соответствующей соты сообщение системы поискового вызова, содержащее МИН вызываемой мобильной станции. Каждая из незанятых мобильных станций М1-М5, которая присутствует в этой соте, будет сравнивать МИН в сообщении системы поискового вызова, принимаемом по каналу управления, с МИН, хранящимся в мобильной станции. Вызываемая мобильная станция с совпадающим МИН автоматически передает ответ системе поискового вызова по каналу управления на базовую станцию, которая затем переадресует ответ системе поискового вызова на ПКМТ 20. Приняв ответ системе поискового вызова, ПКМТ 20 выбирает доступный голосовой канал в соте, из которой был принят ответ поискового вызова (ПКМТ 20 поддерживает для этой цели список незанятых каналов), и запрашивает базовую станцию в этой соте, чтобы приказать мобильной станции через канал управления настроиться на выбранный голосовой канал. Как только мобильная станция настраивается на выбранный голосовой канал, устанавливается сквозное соединение.

С другой стороны, когда вызов инициирован мобильным абонентом (например, путем набора телефонного номера обычного абонента и нажатия кнопки "послать" на телефонной трубке в мобильной станции), набранный номер и пара МИН/ЭСН (электронный серийный номер) для мобильной станции посылаются по каналу управления на базовую станцию и переадресуются на ПКМТ 20, который признает допустимость мобильной станции, присваивает голосовой канал и устанавливает сквозное соединение для разговора, как раскрыто выше. Если мобильная станция перемещается между сотами в состоянии разговора, ПКМТ 20 будет осуществлять передачу обслуживания вызова от старой базовой станции на новую базовую станцию. ПКМТ 20 выбирает доступный голосовой канал в новой соте и затем приказывает старой базовой станции послать на мобильную станцию по текущему голосовому каналу в старой соте сообщение передачи обслуживания, которое информирует мобильную станцию, чтобы она настроилась на выбранный голосовой канал в новой соте.

Сообщение передачи обслуживания посылается в режиме "гашения и выброса", который обуславливает короткий, но весьма заметный перерыв в разговоре. Приняв сообщение передачи обслуживания, мобильная станция настраивается на новый голосовой канал, и ПКМТ 20 устанавливает сквозное соединение через новую соту. Старый голосовой канал в старой соте помечается в ПКМТ 20 как незанятый и может использоваться для другого разговора. Кроме того, при передвижении вне системы обслуживание мобильной станции может быть передано в соту в соседней системе, если между операторами двух систем имеется соглашение о роминге.

Для правильного направления входящих вызовов на мобильную станцию, которая перемещается между различными сотами или системами, необходимо отслеживать местоположение и активность мобильной станции. Для этой цели используется автономный процесс регистрации, в котором мобильная станция посылает системе регистрационное сообщение при вхождении в новую системную зону или в новую зону местоположения (т.е. заранее заданную группу сот в системе) или на заранее определенных интервалах, задаваемых системным оператором. Функции регистрации системной зоны и зоны местоположения можно использовать для идентификации текущего местоположения мобильной станции с тем, чтобы ее поисковый вызов можно было осуществлять в ее фактическом (или наиболее вероятном) местоположении, а не во всех местоположениях в системе. Всякий раз, когда система принимает регистрационное сообщение от мобильной станции в своей зоне, она помечает эту мобильную станцию как активную и присутствующую в ее системной области или в отдельной области местоположения, содержащей соту базовой станции, которая принимала регистрационное сообщение, а затем посылает на эту мобильную станцию сообщение о подтверждении регистрации. Функция периодической регистрации, с другой стороны, используется для определения того,

RU 2190310 C2

RU 2190310 C2

активна ли мобильная станция (включена и находится в высокочастотном диапазоне) в сотовой системе. Входящие вызовы на неактивные мобильные станции могут немедленно маршрутизироваться на записанное сообщение (например, "Мобильный телефон вызываемого вами абонента выключен или находится за пределами области обслуживания. ") без какого-либо поискового вызова этих мобильных станций. Это снижает нагрузку на систему поискового вызова и приводит к более эффективному использованию ограниченной пропускной способности канала управления.

Основные параметры, которые регулируют различные функции мобильной регистрации, включают в себя значение следующей регистрации (СЛРЕГ), которое хранится в каждой мобильной станции, и значения системной идентификации (СИД), идентификации зоны местоположения (ИДЗМП), идентификации регистрации (ИДРЕГ) и инкремента регистрации (ИНКРЕГ), которые транслируются системой по каналу управления каждой соты. СИД - это цифровой номер, который уникально идентифицирует обслуживающую сотовую систему. ИДЗМП - это цифровой номер, который идентифицирует отдельную зону местоположения, состоящую из одной или более сот в системе. ИНКРЕГ задает длину интервала периодической регистрации. ИДРЕГ - это 20-битовый счетчик, который изменяется на единицу при каждом сообщении ИДРЕГ, передаваемом на мобильную станцию. Значение СЛРЕГ указывает, когда ожидается периодическая регистрация, и вычисляется в мобильной станции путем сложения текущих значений ИДРЕГ и ИНКРЕГ. Мобильная станция будет регистрироваться с помощью обслуживающей системы, если либо СИД, либо ИДОМП, принимаемый по каналу управления, отличается от соответствующего значения, которое она сохранила последний раз, когда принимала сообщение о подтверждении регистрации (таким образом, подразумевается, что мобильная станция переместилась в новую зону, соответственно системную или местоположения), или если значение ИДРЕГ, принятое по каналу управления, больше или равно сохраненного СЛРЕГ (таким образом, подразумевается, что ожидается периодическая регистрация). Мобильная станция обновляет значение СПРЕГ (суммой текущих значений ИДРЕГ и ИНКРЕГ) по получении каждого сообщения о подтверждении регистрации и также после каждого успешного назначения голосового канала (т.е. отправки и приемы вызовов рассматриваются как нормальные периодические регистрации, поскольку, производя или принимая вызов, мобильная станция показывает свою активность и местоположение).

Управление доступом любой из мобильных станций М1-М5 к сотовой системе, представленной на фиг. 1, будь то с целью отправки или приема вызова, или же с целью регистрации, осуществляется на основании мобильного идентификационного номера (МИН) и электронного серийного номера (ЭСН), которые хранятся в мобильной станции. МИН идентифицирует абонирование обслуживания и является двоичным представлением 10-значного абонентского телефонного номера мобильного абонента.

МИН присваивается поставщиком сотового обслуживания (оператором собственной системы) и обычно программируется в мобильную станцию либо при приобретении первоначальным пользователем, либо при продаже другому пользователю (т.е. во время постановки на обслуживание). МИН законных (оплачивающих) абонентов сохраняются посредством ПКМТ 20. ЭСН уникально идентифицирует мобильную станцию и является цифровым номером, который выдается производителем и постоянно хранится в мобильной станции (т.е. он установлен фабрично и не подлежит изменению в ходе эксплуатации).

ЭСН мобильных станций, о которых сообщено, что они украдены, могут соответствующим образом помечаться ПКМТ 20, и им навсегда будет отказано в обслуживании.

Кроме МИН и ЭСН, каждая мобильная станция также идентифицируется меткой класса станции (МКС), которая обозначает класс передаваемой мощности, режим и ширину полосы частот для мобильной станции. Мобильные станции в различных классах мощности (портативные, передвижные и автомобильные) будут передавать на одном из нескольких конкретизированных уровнях мощности в пределах различных диапазонов выходной мощности (0,6, 1,6 или 4,0 Вт). Уровень передаваемой мощности в пределах данного диапазона можно увеличивать или уменьшать посредством команды изменения мощности от базовой станции. Кроме того, некоторые мобильные станции способны работать в режиме дискретной передачи (ДП), в котором они могут автономно переключаться между двумя состояниями уровня мощности передатчика ("высокий уровень ДП" и "низкий уровень ДП"). В дополнение, некоторые мобильные станции устанавливаются на работу только в "основном" диапазоне частот, первоначально выделенном сотовым системам, в то время, как другие устанавливаются также на работу в "расширенном" диапазоне частот, который был выделен позже. Подобно МИН и ЭСН необходимая информация МКС хранится в каждой мобильной станции.

Санкционирование пользователя на сотовое обслуживание обычно осуществляется при каждом доступе мобильной станции к системе (т.е. при запросе на регистрацию, при отправке вызова или при ответе системе поискового вызова) посредством мобильной станции. При осуществлении доступа мобильная станция переадресует системе МИН, ЭСН и МКС. ПКМТ 20 поддерживает "белый список", содержащий пары МИН/ЭСН допустимых собственных абонентов и "черный список", содержащий ЭСН краденых или иных несанкционированных мобильных станций. ПКМТ 20 проверяет принятую пару МИН/ЭСН, чтобы определить, принадлежит ли она допустимому собственному абоненту, и если нет, принадлежит ли МИН санкционированному "ромеру" из другой системы и не занесен ли ЭСН в черный

RU 2190310 C2

RU 2190310 C2

список. Если пара МИН/ЭСН не является допустимой, или если МИН не распознается, или если ЭСН занесен в черный список, то мобильной станции может быть отказано в доступе. В противном случае пользователь признается законным и доступ принимается. Предоставляемое затем обслуживание подвергается управлению согласно принимаемой информации МКС.

Первоначальные сотовые системы радиосвязи, как описано в общих чертах выше, использовали аналоговые способы передачи, а именно, частотную модуляцию (ЧМ) и дуплексные (двусторонние) ВЧ-каналы в соответствии со стандартом Усовершенствованная Мобильная Телефонная Служба УМТС. Согласно стандарту УМТС, каждый канал, управляющий или голосовой, между базовой станцией и мобильной станцией использует пару отдельных частот, состоящую из частоты прямой (нисходящей) линии связи для передачи базовой станцией (приема мобильной станцией) и обратной (восходящей) линии связи для передачи мобильной станцией (приема базовой станцией). Система УМТС поэтому является системой с одним каналом на носитель (ОКНН), допускающей только один голосовой тракт (телефонный разговор) на ВЧ-канал. В методике, известной как множественный доступ с частотным разделением (МДЧР), различным пользователям предоставляется доступ к одному и тому же набору ВЧ-каналов, причем каждому пользователю присваивается отдельный ВЧ-канал (пара частот). Эта первоначальная (аналоговая) архитектура УМТС создает основу для промышленного стандарта, внесенного Ассоциацией электронной промышленности (АЭП) и Ассоциацией телекоммуникационной промышленности (АТП), и известного как АЭП/АТП-553 (EIA/TIA-553).

Однако в конце 1980-х гг. сотовая промышленность в Соединенных Штатах начала переходить от аналоговой технологии к цифровой, по большей части в силу необходимости, принимать во внимание устойчивый рост численности абонентов и возрастания спроса на пропускную способность системы. Было выявлено, что повышение пропускной способности, которого добивались для следующего поколения сотовых систем, можно достичь либо путем "дробления сот", чтобы обеспечивать больше каналов на абонентов в конкретных областях, где требуется увеличение пропускной способности, либо путем использования в этих областях более совершенной технологии цифровой радиосвязи, либо путем комбинации обоих подходов. Согласно первому подходу (дробления сот), благодаря уменьшению передаваемой мощности базовой станции размер соответствующей соты (или радиус соты) и вместе с этим расстояние повторного использования частоты уменьшаются, тем самым приводя к увеличению числа каналов на географическую область (т.е. к возрастанию пропускной способности). Дополнительные выгоды от уменьшения размера соты включают в себя увеличение продолжительности "времени разговора" для пользователя, поскольку мобильная станция будет использовать существенно более низкую передаваемую мощность, чем в большей соте, и, следовательно, ее батарею не придется подзаряжать столь же часто.

Хотя дробление сот действительно повысило как пропускную способность, так и покрытие для растущей базы мобильных абонентов, фактический рост пропускной способности ограничивался использованием аналоговой технологии УМТС. Сложилось общее мнение, что желаемый рост пропускной способности и, безусловно, эффективность микросотовой концепции (дробления сот) в увеличении пропускной способности можно максимизировать только путем использования цифровой технологии.

Таким образом, в стремлении перейти к цифровому стандарту, АЭП/АТП (EIA/TIA) разработали некоторое количество стандартов воздушного интерфейса, которые используют методики цифрового кодирования голоса (аналого-цифрового преобразования и уплотнения голоса) и множественного доступа с временным разделением (МДВР) или множественного доступа с кодовым разделением (МДКР), чтобы многократно увеличить число голосовых трактов (переговоров) на ВЧ-канал (т. е. увеличить пропускную способность). Эти стандарты включают в себя (международный стандарт МС) МС-54 [МС-54] (МДВР) и МС-95 (МДКР), которые оба являются "двухрежимными" стандартами, поскольку помимо цифровых речевых каналов, заданных в рамках существующей УМТС, они поддерживают использование аналоговых каналов управления и голоса первоначальной УМТС (с тем, чтобы облегчить переход от аналогового стандарта к цифровому и чтобы дать возможность продолжать использование существующих аналоговых мобильных станций). Двухрежимный стандарт МС-54, в частности, стал известен как стандарт цифровой УМТС (Ц-УМТС). Не так давно АЭП/АТП разработали новую спецификацию для Ц-УМТС, которая включает в себя цифровой канал управления, пригодный для поддержки публичной и личной микросотовой работы, продления срока эксплуатации батареи мобильной станции и увеличения особенностей конечных пользователей. Эта новая спецификация строится на стандарте МС-54Б [IS-54B] (текущее исправление МС-54) и известна как МС-136. (Все предшествующие стандарты АЭП/АТП включены в настоящее описание посредством ссылки, поскольку могут оказаться необходимыми для полного понимания этих разработок, относящихся к предпосылкам изобретения. Копии этих стандартов доступны в Ассоциации электронной промышленности, 2001 Пенсильвания Авеню, С-3., Вашингтон, О.К. 20006 [Electronics Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, D.C. 20006]).

В дополнение к обеспечению нового цифрового формата радиопередачи каждый из стандартов МС-54Б и МС-136 задает процедуру аутентификации для подтверждения идентичности мобильных станций требующих обслуживания в сотовой системе. Эта процедура, которая также была введена в более новые аналоговые стандарты, например, МС-91 для узкополосных УМТС (У-УМТС) и пересмотренная редакция А АЭП/АТП-553

RU 2190310 C2

(АЭП/АТП-553А в настоящее время в разработке), были разработаны в ответ на широко распространенное мошенническое использование пар МИН/ЭСН для кражи сотового обслуживания из существующих аналоговых систем. Многие мобильные станции, проданные до настоящего времени, не отвечают требованию защищенности от краж, предъявляемому к ЭСН, и, следовательно, могут легко программироваться новым ЭСМ (для МИН не существует требования защищенности от краж, и поэтому все мобильные станции легко программируются новыми МИН).

Таким образом, эти мобильные станции могут программироваться, чтобы передавать любую пару МИН/ЭСН с тем, чтобы "обманывать" систему в предоставлении доступа. Дополнительные предпосылки по этому "обрушению" МИН/ЭСН и вытекающим из этого потерь в доходах и обслуживании можно найти в статье под названием "Cellular Fraud" ("Сотовое мошенничество") автора Henry M. Kovalczyk (Генри М. Ковальчик) в Cellular Business, март 1991 г. на стр. 32-35.

Мошенничество в форме переделки МИН/ЭСН возникает, главным образом, в среде "ручного роминга", где сотовые системы не взаимосвязаны на основе реального времени. Поскольку каждый ПКМТ обычно содержал список только допустимых пар МИН/ЭСН, принадлежащих собственным абонентам, он не имел немедленного доступа к спискам двойников в других системах.

Следовательно, используя МИН ромера (т.е. 10-значного абонентского телефонного номера, содержащего код зоны, отличный от местного кода зоны оператора собственной системы) и ЭСН, не занесенный в черный список, мошенническая мобильная станция могла принимать обслуживание от местной сотовой системы до тех пор, пока (возможно, через несколько часов) от собственной системы претендующего ромера (или от разъединяющегося дома) не будет принято указание недопустимости пары МИН/ЭСН. В среде "автоматического роминга", однако, сотовые системы объединены в сеть на основе реального времени в соответствии с положениями стандарта МС-41 АЭП/АТП (или специфического протокола передачи сигналов). Следовательно, обслуживающая сотовая система может получить проверку пары МИН/ЭСН от собственной системы виртуально немедленно и может поэтому без существенной задержки отказать в обслуживании переделке МИН/ЭСН.

Недавно появился тип мошенничества, известный как "клонирование", в котором мошеннический пользователь заимствует подлинную пару МИН/ЭСН допустимого (оплачивающего) абонента. Мошеннический пользователь может тем или иным путем тайно завладеть подлинной парой МИН/ЭСН или даже списком допустимых пар МИН/ЭСН. Например, в некоторых случаях подлинные номера МИН/ЭСН печатаются на ярлыке, прикрепленном к мобильной станции, принадлежащей действительному абоненту, и их можно прочитать. В других случаях список подлинных пар МИН/ЭСН может быть куплен на "черном рынке" или непосредственно у служащего сотового оператора. В дополнение, поскольку каждая мобильная станция передает пару МИН/ЭСН на обслуживающий обмен при каждом доступе в систему, одна или более подлинных пар МИН/ЭСН могут быть перехвачены путем прослушивания радиопередач на (аналоговом) канале управления.

Процедуры аутентификации в более новых промышленных стандартах стремятся найти различие между законными мобильными станциями и мошенническими клонами через синхронизованную генерацию криптопеременных из идентичных наборов коллективных секретных данных (КСД), которые хранятся и периодически обновляются в мобильной станции и ее обслуживающей базовой станции. Мобильная станция и базовая станция обмениваются между собой этими криптопеременными с целью подтверждения идентичности мобильной станции. Поскольку считается, что клоновая мобильная станция не имеет доступа к первоначальному значению КСД или последующей истории обновлений КСД в законной мобильной станции, ее криптопеременные не будут совпадать с криптопеременными базовой станции и потому ее можно будет идентифицировать как клон. КСД для каждой мобильной станции хранится в ПКМТ собственной системы или в отдельной абонентской базе данных, именуемой "домашним регистром" (ДР), который подключается к этому ПКМТ и предоставляется обслуживающей базовой станции. Каждая мобильная станция также хранит в памяти свои КСД.

В процессе аутентификации базовая станция генерирует и посылает на мобильную станцию произвольную кодовую комбинацию битов, именуемую ПККБ (RAND) или ПККБУ (RANDU), по аналоговому каналу управления (АКУ), цифровому каналу управления (ЦКУ), аналоговому голосовому каналу (АГК) или каналу цифрового графика (КЦТ). И мобильная станция, и базовая станция используют ПККБ или ПККБУ, часть КСД, именуемую КСД-А (оставшаяся часть, КСД-Б, используется для шифрования, а не для аутентификации), совместно с другими параметрами (например, МИН и ЭСН мобильной станции) в качестве входных переменных алгоритма сотовой аутентификации и шифрования голоса (САШГ), который задан в Приложении А к каждому из стандартов МС-54Б и МС-136, чтобы генерировать аутентификационный ответ, именуемый АУТО (AUTHR) или АУТУ (AUTHU) (в зависимости от того, используется ли соответственно ПККБ или ПККБУ). Аутентификационный ответ вычисляется в мобильной станции и посылается на базовую станцию для сравнения с аутентификационным ответом, вычисленным на базовой станции. Если аутентификационные ответы совпадают, аутентификация признается успешной (т. е. считается, что базовая станция и мобильная станция имеют идентичные наборы КСД). Однако, если сравнение на базовой станции дает отрицательный результат, базовая станция может отказать мобильной станции в обслуживании или начать процесс обновления КСД.

Процедура для обновления КСД для любой мобильной станции предполагает применение САШГ, инициализированного информацией специфики мобильной станции

RU 2190310 C2

RU 2190310 C2

(ЭСН) определенными произвольными данными (ПРОИЗКСД) и секретным, неизменным ключом аутентификации (А-ключом), который уникально присваивается мобильной станции. По соображениям безопасности, А-ключ никогда не передается по воздушному интерфейсу между базовой станцией и мобильной станцией или по сетевому интерфейсу между различными сотовыми системами. А-ключ хранится в ПКМТ или ДР и должен вводиться в память мобильной станции для использования в обновлении КСД. А-ключ может вводить в мобильную станцию санкционированный техник при активации мобильного обслуживания, используя режим программирования стандартного модуля присвоения номера (МПН), или мобильный абонент, в любое время используя отдельный режим программирования А-ключа, как изложено в Патенте США 5551073. Для любых мобильных станций, имеющих множественные МПН и использующих множественные МИН (т.е. где пользователь абонирует обслуживание у множественных собственных систем с целью избежать расходов ромера в этих системах), множественные А-ключи могут подлежать вводу в мобильную станцию по одному на каждый МПН (МИН). Для каждого МИН следует вводить различные А-ключи, поскольку, по соображениям безопасности, А-ключ может быть известен только мобильной станции и ПКМТ или ДР собственной системы и не должен передаваться от системы к системе при роминге мобильной станции. Таким образом, обновления КСД (в которых А-ключ используется, чтобы генерировать новые значения КСД) выполняются только в мобильной станции и связанном с нею ПКМТ или ДР собственной системы, который затем посылает значения КСД (но не А-ключ) на обслуживающую систему).

Вследствие важности А-ключа для целей аутентификации организация безопасности выдачи А-ключа имеет промышленное значение. Первоначально представлялось, что каждая мобильная станция должна отправляться с фабрики с А-ключом, по умолчанию состоящим из всех двоичных нулей, и что действующее значение для А-ключа будет присваиваться системным оператором, когда мобильный абонент подлишется на обслуживание. Присвоенное значение А-ключа затем вводилось бы служебным техником или пользователем. Однако, по причине административного бремени и угрозы безопасности, связанной с доставкой (например, по почте) многочисленных А-ключей служебным техникам или мобильным абонентам, сочли более предпочтительным, чтобы производители мобильных станций отправляли каждую из мобильных станций с произвольным значением А-ключа. Любой производитель затем мог бы обеспечивать любого системного оператора списком комбинаций ЭСН/произвольный А-ключ, например, в защищенной базе данных. Значения А-ключей из этого списка, в свою очередь, подвергались бы программированию в ПКМТ или ДР собственной системы и использовались бы системным оператором для аутентификации соответствующих мобильных станций.

В настоящем и в ближайшем обозримом будущем оба вышеизложенных подхода к организации А-ключа (А-ключ, принятый по умолчанию, и произвольный А-ключ) используются и, как ожидается, будут использоваться в сотовой промышленности. Некоторые операторы руководствуются подходом А-ключа, принятого по умолчанию, по причине его простоты и/или по причине неспособности некоторых ПКМТ программироваться конкретными значениями А-ключа (произвольными или какими-либо еще) для всех различных абонентов. Некоторые из этих операторов даже прибегли к переустановке А-ключей на значение, принятое по умолчанию, во всех случаях, включая те, в которых А-ключ мог быть первоначально установлен на произвольное значение. Другие операторы, однако, предпочитают использовать подход произвольного А-ключа по причине его дополнительной безопасности.

Иные операторы, стремящиеся к дополнительной безопасности, сознают, что список ЭСН/произвольный А-ключ может стать избыточным, не организуемым или поврежденным, и что для мобильных станций с множественными МПН один и тот же произвольный А-ключ будет доступен множественным носителям, таким образом, ставя под угрозу безопасность (если только производитель не пожелает программировать различные произвольные значения А-ключа для различных МПН, в таком случае список ЭСН/А-ключ может стать еще больше). Такие операторы могут предпочесть иметь индивидуальный (клиентский) А-ключ, присваиваемый мобильному абоненту в момент активации обслуживания для ввода в его мобильную станцию.

Исходя из предпосылок изобретения и склонности некоторых абонентов переключаться между различными поставщиками услуг (операторами), возможно, ведущими различную политику в организации А-ключей, очевидно необходима такая процедура организации А-ключа, которая объединяла бы имеющиеся подходы и в то же время была бы свободна от присущих им недостатков, таких, как стоимость поддержания списков произвольных А-ключей для мобильных станций от каждого производителя.

Сущность изобретения

Настоящее изобретение допускает в ходе программирования МПН мобильной станции выбор А-ключа из различных возможностей, а именно, значений, принимаемых по умолчанию, произвольных и пользовательских. Если желаемым является значение, принимаемое по умолчанию, А-ключ может быть установлен равным этому значению в ходе эксплуатации, а не только во время изготовления мобильной станции. Аналогично, если выбирается произвольное значение, это значение может генерироваться внутренне в мобильной станции с использованием набора входных данных и алгоритма, которые также доступны собственной системе.

Альтернативно, произвольное значение может предварительно вычисляться производителем с использованием такого алгоритма и затем сохраняться в мобильной

RU 2190310 C2

RU 2190310 C2

станции для возможного выбора в качестве А-ключа. Таким образом, собственной системе или производителю мобильной станции не требуется поддерживать список ЭСН/произвольные значения А-ключа, поскольку можно использовать заранее заданный алгоритм, чтобы получить дубликат произвольного значения А-ключа, генерируемого или предварительно сохраненного в мобильной станции. Кроме того, если мобильная станция, отвечающая настоящему изобретению, вынуждена переключать абонирования от собственной системы, которая предпочитает использовать произвольный А-ключ, к новой собственной системе, которая предпочитает использовать А-ключ, принятый по умолчанию, то А-ключ, хранящийся в мобильной станции, можно легко переустановить от произвольного значения А-ключа к значению, принятому по умолчанию (и наоборот). Если всякий раз подлежит использованию клиентский А-ключ, настоящее изобретение также обеспечивает простоту ввода в мобильную станцию такого А-ключа.

В одном своем аспекте настоящее изобретение предоставляет способ конфигурирования мобильной станции с ключом аутентификации (А-ключа), который хранится в памяти мобильной станции. Способ содержит этапы разрешения мобильной станции принимать команду, вводимую пользователем для выбора из множества возможных значений А-ключа, включающих в себя значение, задаваемое по умолчанию, и случайное значение; установления А-ключа в памяти на значение, задаваемое по умолчанию, если команда указывает на выбор значения, задаваемого по умолчанию; и установления А-ключа в памяти на случайное значение, если команда указывает на выбор случайного значения. Случайное значение может быть выработано в мобильной станции в ответ на команду, указывающую на выбор случайного значения, или альтернативно оно может являться предварительно генерированным случайным значением, которое хранится в мобильной станции для использования в качестве А-ключа, если команда указывает на выбор случайного значения.

В другом случае случайное значение А-ключа может генерироваться из входных данных, включающих в себя электронный серийный номер (ЭСН) мобильной станции и системную идентификацию собственной системы (СИДС) мобильной станции, таким образом обеспечивая разное случайное значение А-ключа для каждой мобильной станции и для каждого МПН, хранящегося в мобильной станции. Кроме того, согласно этому способу, возможные значения А-ключа могут дополнительно включать в себя клиентское значение, подлежащее вводу пользователем, а способ может дополнительно содержать этап установления А-ключа в памяти на клиентское значение, вводимое пользователем, если команда указывает на выбор клиентского значения. Команда, будь то для выбора значения А-ключа, задаваемого по умолчанию, случайного или клиентского, может быть введена в ходе программирования модуля присвоения номера (МПН) мобильной станции.

В другом аспекте настоящее изобретение обеспечивает мобильную станцию, содержащую в себе память для хранения значения ключа аутентификации (А-ключа), средство ввода команды выбора из множества возможных значений А-ключа, включая в себя значение, задаваемое по умолчанию, и случайное значение; средство установления А-ключа в памяти на значение, задаваемое по умолчанию, если команда указывает на выбор значения, задаваемого по умолчанию; и средство установления А-ключа в памяти на случайное значение, если команда указывает на выбор случайного значения.

Согласно этому аспекту возможные значения А-ключа могут дополнительно включать в себя значение, вводимое пользователем, и мобильная станция может дополнительно содержать средство установления А-ключа в памяти на значение, вводимое пользователем, если команда указывает на выбор значения, вводимого пользователем. Мобильная станция может дополнительно содержать средство отображения списка возможных буквенно-цифровых идентификаций для вводимого пользователем значения А-ключа, причем из этого списка буквенно-цифровая идентификация может быть выбрана для сохранения в памяти вместе с вводимым пользователем значением А-ключа.

Сохраненное значение А-ключа может быть затем вновь вызвано из памяти и отображено с использованием его буквенно-цифровой идентификации, вместо того, чтобы отображать его фактическое значение, которое, в целях безопасности, должно оставаться скрытым от обозрения.

Эти и другие аспекты, предметы и преимущества настоящего изобретения очевидны из нижеследующего подробного описания подробного описания и чертежей, на которых

фиг. 1 - архитектура общепринятой сотовой системы радиосвязи, включающей в себя совокупность мобильных станций и базовых станций;

фиг. 2 - упрощенная блок-схема мобильной станции, которая может быть использована в соответствии с настоящим изобретением;

фиг. 3 - блок-схема информационного блока МПН, хранящегося в ЭППЗУ (электроперепрограммируемое постоянное запоминающее устройство) мобильной станции, представленной на фиг. 2; и

фиг. 4 - алгоритм выбора А-ключа и этапов сохранения исполняемых мобильной станцией, представленной на фиг. 2, в соответствии с настоящим изобретением.

На фиг. 2 представлена упрощенная блок-схема мобильной станции 100, которую можно использовать в соответствии с настоящим изобретением. Мобильная станция 100 содержит микрофон 102, громкоговоритель 104, клавиатуру или клавишную панель 106, буквенно-цифровой или графический дисплей 108, интерфейс 110 пользователя, микропроцессор 112, программную память 114, оперативную память (ОЗУ) 116, электроперепрограммируемое постоянное запоминающее устройство (ЭППЗУ) 118, высокочастотную (ВЧ) секцию 120 и антенну

RU 2190310 C2

RU 2190310 C2

122.

Интерфейс пользователя 110 содержит схему обработки речи и данных (не показана), например, кодер-декодер для осуществления аналого-цифрового преобразования (АЦП) передаваемого речевого сигнала от микрофона 102 и цифроаналогового преобразования (АЦП) принимаемого речевого сигнала, предназначенного для громкоговорителя 104. Интерфейс 110 пользователя дополнительно содержит цифровой сигнальный процессор (ЦСП) для осуществления усиления/ослабления, фильтрации, уплотнения/разуплотнения, кодирования/декодирования канала и любой другой желаемой обработки (например, в соответствии с МС-136) речи и данных пользователя или управления.

ВЧ-секция 120 содержит схему ВЧ-обработки (не показана), например, ВЧ-передатчик для модулирования передаваемой речи или данных в аналоговый сигнал носителя, преобразования с повышением частоты модулированного сигнала до частоты выбранного канала и последующих фильтрации, усиления и передачи сигнала через антенну 122. ВЧ-секция 120 дополнительно содержит ВЧ-приемник для преобразования с понижением частоты модулированного сигнала, принимаемого через антенну 122 в сигнал промежуточной частоты (ПЧ) и последующих фильтрации и демодулирования ПЧ-сигнала для дополнительной обработки в ЦСП.

Микропроцессор 112 управляет всей работой мобильной станции 100 посредством программ программного обеспечения, хранящихся в программной памяти 114. Эти программы включают в себя, например, исполняемые инструкции для операций как передачи, так и приема на цифровом канале управления (ЦКУ) и канале цифрового графика (КЦТ), что конкретизировано в МС-136. ОЗУ 116 удерживает значения временных переменных, используемых при исполнении этих инструкций. Параметры, значения которых должны сохраняться после выключения питания в мобильной станции 100, будут храниться в ЭППЗУ 118 (или в аналогичной энергонезависимой или флэш-памяти). Такие параметры включают в себя мобильный идентификационный номер (МИН), электронный серийный номер (ЭСН) мобильной станции 100, метку класса станции (МКС), системную идентификацию собственной системы (СИДС) и ключ аутентификации (А-ключ).

На фиг. 3 представлена блок-схема информационного блока модуля присвоения номера (МПН), который хранится в ЭППЗУ 118 в соответствии с настоящим изобретением.

В ходе программирования МПН служебный техник, санкционированный сотовым носителем (оператором), вводит в мобильную станцию значения определенных специфических параметров абонента, мобильной станции и системы с целью установить и конфигурировать мобильную станцию для работы в системе этого носителя. Как показано на фиг. 3, типичный информационный блок МПН включает в себя МИН, МКС и СИДС (которые являются специфическими для соответственно абонента, мобильной станции и системы), а также другие параметры, которые конкретно не показаны на фиг.3.

В случае абонентов, которые подписались на обслуживание у множественных носителей, ЭППЗУ 118 будет содержать информационные блоки множественных МПН, подобные представленному на фиг.3, по одному на каждый из этих носителей. Очевидно, что хотя каждый из параметров на фиг.3 показан содержащимся в одной области памяти, на практике разные части значения любого параметра могут храниться в различных областях памяти, что обусловлено размером памяти и другими ограничениями.

Как представлено на фиг. 3, информационный блок каждого МПН в мобильной станции 100 включает в себя значение А-ключа, который, по соображениям безопасности, может быть закодирован или зашифрован и/или распределен по нескольким областям памяти внутри блока соответствующего МПН. Согласно настоящему изобретению, это значение А-ключа может быть значением "задаваемым по умолчанию" (все нули), "случайным" (генерированным случайным образом) значением или "клиентским" (задаваемым пользователем) значением. Кроме того, как показано на фиг. 3, информационный блок МПН может включать в себя значение "начальное число", которое может быть использовано при генерировании случайного значения А-ключа в соответствии с настоящим изобретением. Выбор и хранение желаемого А-ключа дополнительно раскрыты ниже.

На фиг. 4 представлен алгоритм выбора А-ключа и процедуры сохранения, осуществляемых мобильной станцией в соответствии с настоящим изобретением. Эта процедура инициируется пользователем, вызывающим на этапе 200 режим программирования МПН. Пока программируется МПН, дисплей 108 приглашает пользователя ввести значения параметров в блок отдельного МПН (т.е. связанного с отдельным сотовым оператором). Таким образом, например, пользователь на этапе 202 может ввести с клавиатуры 106 МИН и СИДС, предназначенные отдельной "домашней" системой или для нее с целью сохранения в блоке соответствующего МИН (как показано на фиг.3). После того, как значения этих (и, возможно, других) параметров введены, дисплей 108 приглашает пользователя на этапе 204 выбрать вариант А-ключа, задаваемого по умолчанию, случайного А-ключа или клиентского А-ключа, или же, альтернативно, добавить буквенно-цифровую метку к текущему А-ключу, хранящемуся в блоке МПН.

Если на этап 204 пользователь выбрал вариант А-ключа, задаваемого по умолчанию, А-ключ в блоке МПН на этапе 206 будет установлен на нулевое значение. Однако, если на этапе 204 пользователь выбрал вариант случайного А-ключа, то на этапе 208 будет генерироваться псевдослучайный А-ключ, исходя из СИДС, введенного в ходе программирования МПН, ЭСН мобильной станции и, возможно, значения "начального числа". Значение "начальное число" может быть любым значением, доступным как в

RU 2190310 C2

мобильной станции, так и в системе, например, значением ПККБ или ИДРЕГ, передаваемым по каналу управления или, альтернативно, предварительно определенным значением, хранящимся или генерируемым как в мобильной станции, так и в системе. СИДС, ЭСН и/или начальное число используются как входные переменные для алгоритма САШГ или другого алгоритма, который способен генерировать псевдослучайное значение А-ключа с нормальным распределением. Псевдослучайное значение А-ключа, генерируемое в соответствии с этим алгоритмом, на этапе 210 сохраняется в блоке соответствующего МПН.

В альтернативном варианте осуществления настоящего изобретения псевдослучайное значение А-ключа может быть предварительно вычислено для любой комбинации СИДС/ЭСН в фабричных условиях с использованием алгоритма, подобного вышеописанному. Например, отдельный сотовый оператор может заказать у производителя некоторое количество мобильных станций, с оговоркой, что все они будут иметь случайные значения А-ключа. Тогда производитель может использовать СИДС этого оператора и ЭСН каждой мобильной станции, чтобы генерировать соответствующее случайное значение А-ключа, которое сохраняется в памяти мобильной станции. В этом случае, когда пользователь на этапе 204 выбирает вариант случайного А-ключа, сохраненное значение А-ключа будет записано в соответствующую ячейку в блоке МПН, как показано на фиг. 3. Очевидно, что для мобильной станции с множественными МПН множественные случайные значения А-ключа можно предварительно вычислять и сохранять в памяти мобильной станции, по одному А-ключу на каждый МПН. Таким образом, после того, как пользователь на этапе 202 ввел необходимые значения в блок отдельного МПН и затем на этапе 204 выбрал вариант случайного А-ключа, как показано на фиг. 4, сохраненное случайное значение А-ключа, связанное с этим МПН, будет записано в блок соответствующего МПН.

Очевидно, что генерирование случайного А-ключа (или точнее "псевдослучайного" А-ключа, поскольку он генерируется алгоритмом), в соответствии с настоящим изобретением, освобождает от необходимости поддержания списка ЭСН/случайный А-ключ для всех мобильных станций, произведенных каждым производителем, и связанных с этим затрат, поскольку и производитель, и собственная система может вычислять случайное значение А-ключа для любой мобильной станции в любой момент с использованием заранее определенных входных данных (например, СИДС, ЭСН и/или начального числа) в заранее определенном алгоритме (например, САШГ). Кроме того, поскольку ЭСН любой мобильной станции уникален, каждая мобильная станция будет иметь уникальное случайное значение А-ключа, таким образом увеличивая безопасность системы. В дополнение, поскольку СИДС любой системы уникален, значение случайного А-ключа (которое также основывается на СИДС) будет различаться для каждого абонирования (блока МПН), поддерживаемого одной и той же мобильной станцией (ЭСН). Другими словами, различные "собственные" носители для одной и той же мобильной станции будут использовать различные случайные значения А-ключа, таким образом дополнительно увеличивая безопасность благодаря исключению необходимости в совместном использовании одного и того же значения А-ключа среди этих носителей.

Возвращаясь к этапу 204, пользователь может выбрать вариант ввода в блок текущего МПН особого (клиентского) А-ключа. На этапе 212 пользователь вводит цифры А-ключа через клавиатуру 106. Допустимость этих цифр оценивается на этапе 214 посредством процедуры проверки, которая конкретизируется, например, в Приложении А к каждому из стандартов МС-54 и МС-136. Как только введенный А-ключ признается допустимым, он сохраняется в блоке текущего МПН на этапе 216. Затем, на этапе 218 список буквенно-цифровых меток появляется на дисплее 108 с тем, чтобы пользователь мог выбрать одну из этих меток, чтобы она служила идентификацией для только что введенного А-ключа. Этот этап позволяет пользователю позднее повторно вызвать и отобразить А-ключ с использованием его идентификации, поскольку сам А-ключ не подлежит отображению по соображениям безопасности. Метка будет информировать пользователя, что текущий А-ключ в блоке соответствующего МПН не является ни задаваемым по умолчанию, ни случайным А-ключом, но является клиентским значением А-ключа, которое было предварительно сохранено в блоке этого МПН. В общем случае метка может быть любой заранее заданной буквенно-цифровой строкой, например датой последнего ввода клиентского значения А-ключа. Как только пользователь выбирает метку, она сопоставляется с хранящимся А-ключом на этапе 220.

Если на этапе 204 пользователь выбрал вариант ввода метки для текущего А-ключа, хранящегося в блоке МПН, значение этого А-ключа, которое могло быть предварительно введено с использованием отдельной процедуры ввода А-ключа, как описано в Патенте США 5551073, не будет изменено, и процедура просто перейдет к этапам 218-220 выбора и сохранения соответствующей метки.

Вышеприведенное подробное описание показывает только определенные конкретные варианты осуществления настоящего изобретения. Специалистам очевидно, что многие модификации и вариации могут быть выполнены без существенного выхода за рамки настоящего изобретения. Соответственно, форма изобретения, описанная здесь, является только иллюстративной и не предполагается как ограничение объема настоящего изобретения, определяемого формулой изобретения.

Формула изобретения:

1. Способ конфигурирования мобильной станции (100) с ключом аутентификации (А-ключа), который хранится в памяти (118) упомянутой мобильной станции (100), содержащий этапы разрешения упомянутой мобильной станции (100) принимать команду

RU 2190310 C2

(204), вводимую пользователем для выбора из множества возможных типов значений упомянутого А-ключа, включающих в себя значение, задаваемое по умолчанию, и случайное значение, установления (206) упомянутого А-ключа в упомянутой памяти (118) на упомянутое значение, задаваемое по умолчанию, если упомянутая команда (204) указывает на выбор упомянутого значения, задаваемого по умолчанию, и установления (208-210) упомянутого А-ключа в упомянутой памяти (118) на упомянутое случайное значение, если упомянутая команда (204) указывает на выбор упомянутого случайного значения.

2. Способ по п. 1, при котором упомянутую команду вводят в ходе программирования (200) модуля присвоения номера (МПН) упомянутой мобильной станции.

3. Способ по п. 1, при котором упомянутое значение, задаваемое по умолчанию, является нулевым.

4. Способ по п. 1, при котором упомянутое случайное значение является функцией заранее определенных данных, включающих в себя электронный серийный номер (ЭСН) упомянутой мобильной станции (100).

5. Способ по п. 4, при котором упомянутые данные дополнительно включают в себя системную идентификацию домашней системы (СИДС) упомянутой мобильной станции (100).

6. Способ по п. 4, при котором упомянутые данные дополнительно включают в себя заранее определенное значение начального числа.

7. Способ по п. 1, при котором упомянутые возможные значения А-ключа дополнительно включают в себя клиентское значение, подлежащее вводу упомянутым пользователем, а способ дополнительно содержит этап установления (212-216) упомянутого А-ключа в упомянутой памяти (118) на клиентское значение, введенное упомянутым пользователем, если упомянутая команда (204) указывает на выбор упомянутого клиентского значения.

8. Способ по п. 7, при котором упомянутое клиентское значение признается допустимым (124) после его ввода (212) упомянутым пользователем и перед установлением (216) упомянутого А-ключа в упомянутой памяти (118) на упомянутое клиентское значение. ,

9. Способ по п. 7, дополнительно содержащий этап разрешения упомянутой мобильной станции (100) принимать буквенно-цифровую идентификацию (218) упомянутого клиентского значения, введенного упомянутым пользователем для сохранения (220) с упомянутым клиентским значением в упомянутой памяти (118).

10. Мобильная станция (100), содержащая память (118) для хранения значения ключа аутентификации (А-ключа), средство (106, 110) ввода команды (204) для выбора из множества возможных типов значений для упомянутого А-ключа, включающих в себя значение, задаваемое по умолчанию, и случайное значение, средство (112, 206) установления упомянутого А-ключа в упомянутой памяти (118) на упомянутое значение, задаваемое по умолчанию, если упомянутая команда (204) указывает на выбор упомянутого значения, задаваемого по умолчанию, и средство (112, 208-210) установления упомянутого А-ключа в упомянутой памяти (118) на упомянутое случайное значение, если упомянутая команда (204) указывает на выбор упомянутого случайного значения.

11. Мобильная станция по п. 10, в которой упомянутая память (118) содержит электроперепрограммируемое постоянное запоминающее устройство (ЭППЗУ).

12. Мобильная станция по п. 10, в которой упомянутое средство ввода команды содержит буквенно-цифровую клавиатуру (106).

13. Мобильная станция по п. 10, в которой упомянутую команду (204) вводят в ходе программирования (200) модуля присвоения номера (МПН) упомянутой мобильной станции (100).

14. Мобильная станция по п. 10, в которой упомянутое значение, задаваемое по умолчанию, является нулевым.

15. Мобильная станция по п. 10, в которой упомянутое случайное значение является функцией заранее определенных данных, включающих в себя электронный серийный номер (ЭСН) упомянутой мобильной станции (100).

16. Мобильная станция по п. 15, в которой упомянутые данные дополнительно включают в себя системную идентификацию домашней системы (СИДС) упомянутой мобильной станции (100).

17. Мобильная станция по п. 15, в которой упомянутые данные дополнительно включают в себя заранее определенное значение начального числа.

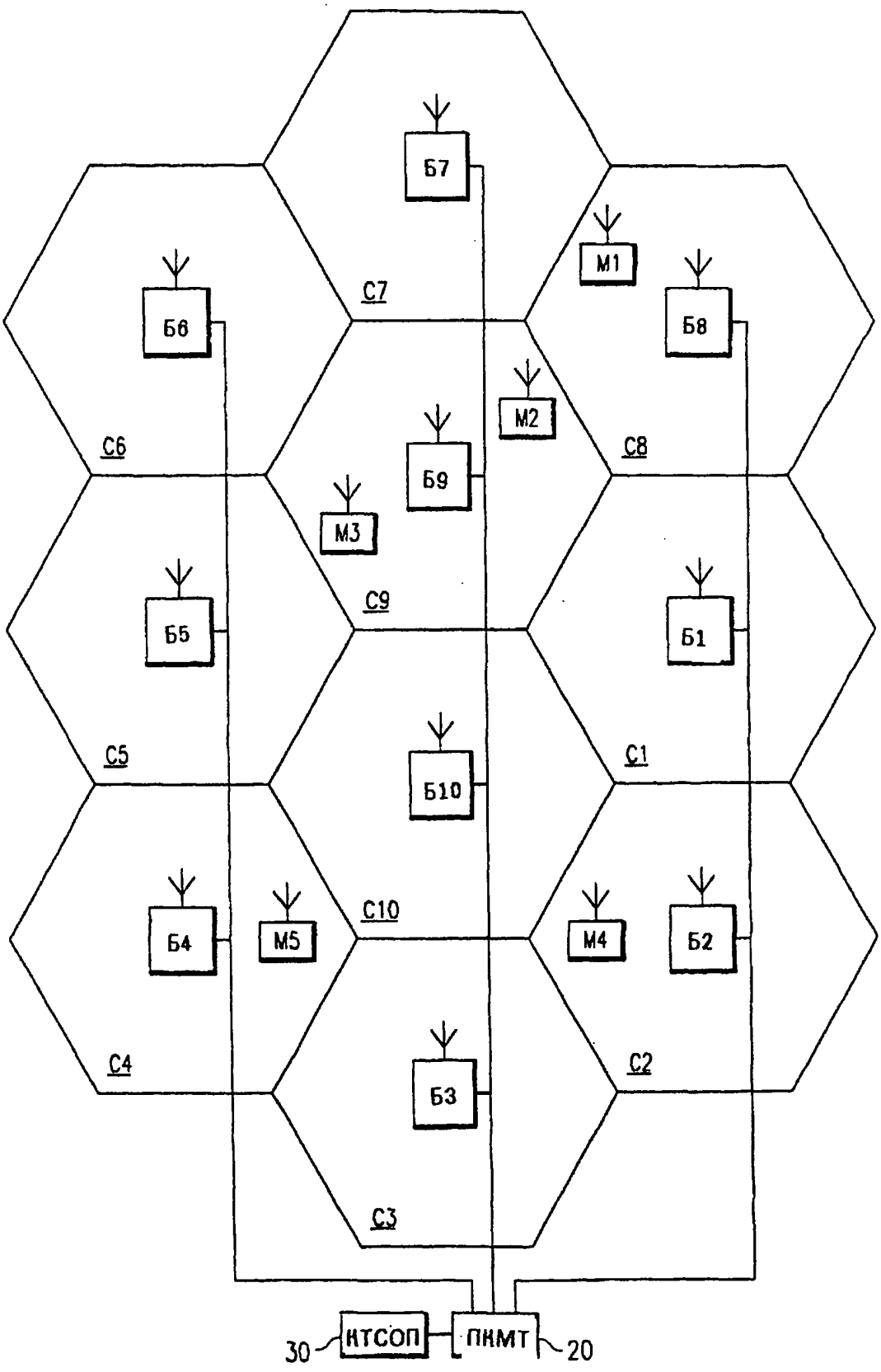
18. Мобильная станция по п. 10, в которой упомянутые возможные значения А-ключа дополнительно включают в себя вводимое пользователем значение, а упомянутая мобильная станция дополнительно содержит средство (112, 212-216) установления упомянутого А-ключа в упомянутой памяти (118) на упомянутое вводимое пользователем значение, если упомянутая команда (204) указывает на выбор упомянутого вводимого пользователем значения.

19. Мобильная станция по п. 18, в которой упомянутое вводимое пользователем значение признается допустимым (214) до установления упомянутого А-ключа в упомянутой памяти (118) на упомянутое вводимое пользователем значение.

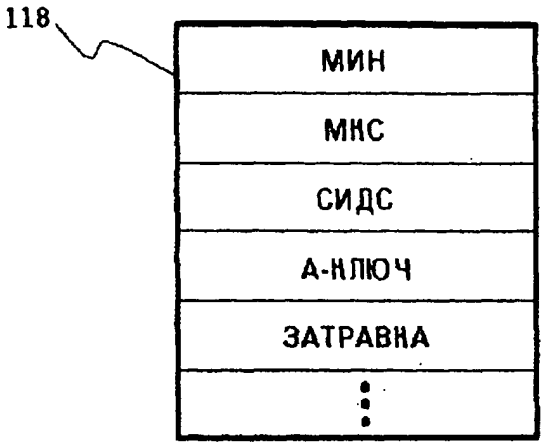
20. Мобильная станция по п. 18, дополнительно содержащая средство (108) отображения списка возможных буквенно-цифровых идентификаций (218) упомянутого вводимого пользователем значения А-ключа, причем из этого списка буквенно-цифровая идентификация может быть выбрана для сохранения (220) с упомянутым вводимым пользователем значением А-ключа в упомянутой памяти (118).

RU 2190310 C2

RU 2190310 C2

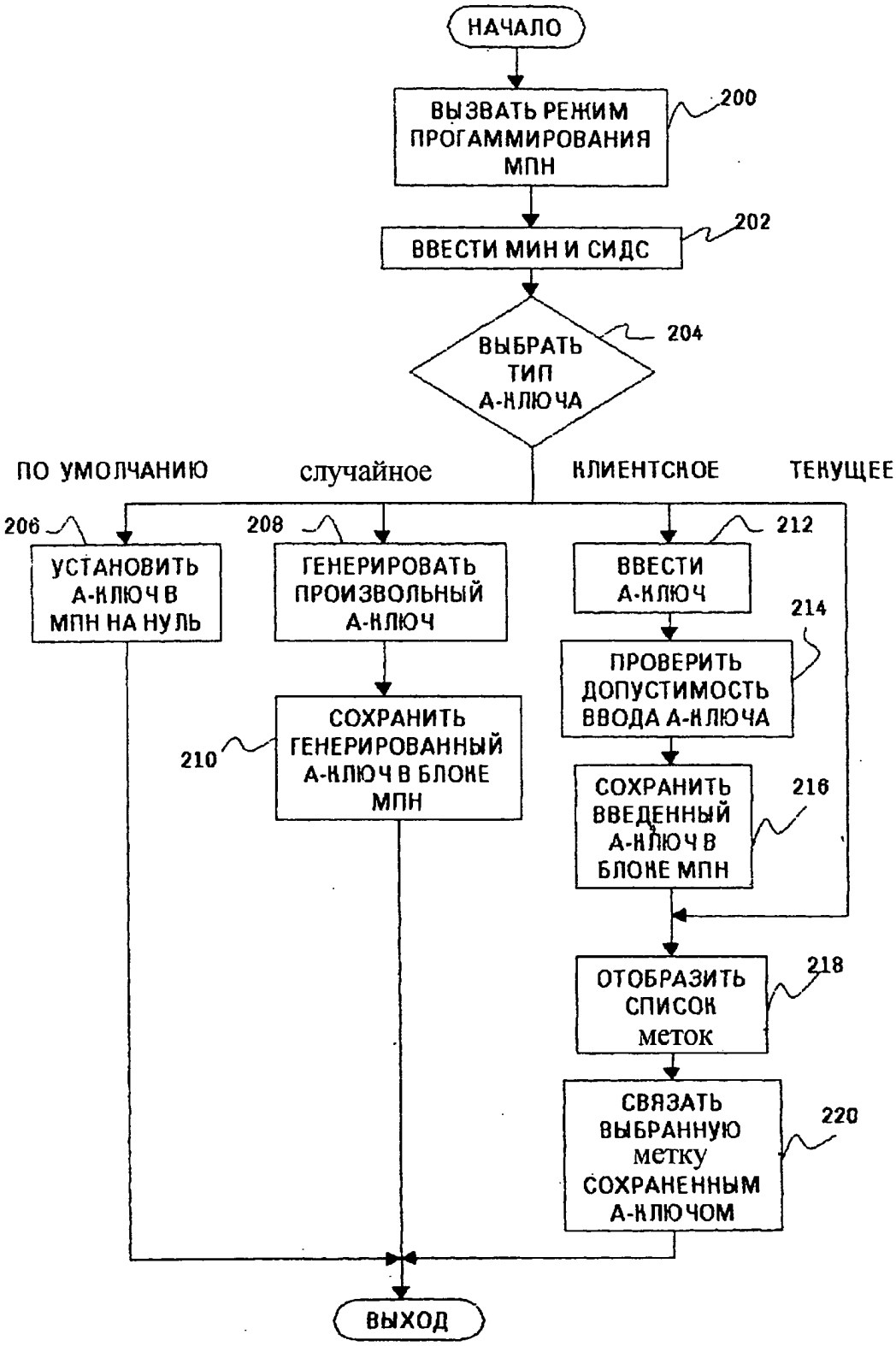


Фиг. 1



Фиг. 3

RU 2190310 C2



Фиг. 4

RU 2190310 C2